Governance & Management

Description

Governance and management of security are most effective when they are systemic, woven into the culture and fabric of organizational behaviors and actions. They create and sustain connections among principles, policies, processes, products, people, and performance.

This means that security must come off the technical sidelines and not be relegated to software development and IT departments. Boards of directors, senior executives, and managers all must work to establish and reinforce a relentless drive toward effective enterprise security. If the responsibility for enterprise security is assigned to someone who lacks the authority, accountability, and resources to enforce it, the desired level of security will not be articulated, achieved, or sustained. Even the best efforts to buy secure software and build security into developed software meet "considerable resistance because the problem is mostly organizational and cultural, not technical" [Steven 06][1].

This shift in perspective elevates security to more than just a standalone technical concern. Because security is now a business problem and not a technical backwater, the organization must activate, coordinate, deploy, and direct many of its core competencies to create effective solutions. And to sustain success, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [Caralli 04b][2].

The objective of this content area is to aid software developers and their managers, and security professionals and their managers, to more effectively engage their leaders and executives on security governance and management. The intent is to build attentive, security-conscious leaders who are in a better position to make well-informed security investment decisions across the software and system development life cycle.

Articles in this Content Area

The articles in this content area provide a recommended order of steps to tackle to govern and manage enterprise security.

1. The overview, "Security Is Not Just a Technical Issue[3]," defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.
2. The second article, "Framing Security as a Governance and Management Concern: Risks and Opportunities[4]," briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs.
3. The third article, "How Much Security Is Enough?[5]," provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and criteria for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.
4. The fourth article, "Maturity of Practice and Exemplars[6]," identifies several indicators that

1. daisy:564#wp1012305 (Governance and Management References)
2. daisy:564#wp1012153 (Governance and Management References)
3. daisy:563 (Security Is Not Just a Technical Issue)
4. daisy:565 (Framing Security as a Governance and Management Concern: Risks and Opportunities)
5. daisy:566 (How Much Security Is Enough?)
6. daisy:567 (Maturity of Practice and Exemplars)

organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.

5. The fifth article, "Adopting an Enterprise Security Framework[7]," by John Steven, originally appeared in *IEEE Security & Privacy*. It describes a suggested approach for putting an enterprise security program in place, including necessary governance and management actions. According to Steven, "Put simply, without executive sponsorship, a unified understanding of roles, responsibilities, and a vision for software security, the effort will sink quickly into political struggle or inaction."

The first four articles draw from a wide range of technical reports, other materials, external sources, and collaborators who are successfully addressing this topic. They summarize CERT field work and applied research conducted over the past two years. Much of this content draws from and is expanded in [Allen 05][8].

Notes to the Reader

The articles in this content area

- address security at the enterprise and organizational level, *not* at the system or software level. CERT research and field experience indicate that enterprise-level action is necessary to achieve and sustain secure systems and software and protect the security of information. This includes the commitment and action to address security throughout the software development life cycle.
- are written for security professionals and their managers, seeking to more effectively engage their leaders and executives in security governance and management
- intentionally do not clearly distinguish between security governance and security management. Typically, governance is responsible for direction, control, and oversight, and management is responsible for execution. The roles and distinctions vary widely by type of organization and the market sector within which an organization operates.
- do not provide detailed "how-to" guidance. The fourth and fifth articles provide exemplars and frameworks to consider. Articles in other BSI content areas provide more details to help enact the recommendations presented here. These include Acquisition, Architectural Risk Analysis[9], Architecture, Assembly, Integration, and Evolution[10], Business Case[11], Incident Management[12], Measurement[13], Principles[14], Project Management[15], Risk Management[16], SDLC Process[17], Software System Policy, and Strategies.

Podcasts on Enterprise Security

"Security for Business Leaders[18]" is a series of conversations that provide both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be.

Overview Articles

Name	Version Creation Time	Abstract
Security is Not Just a Technical Issue	11/9/06 5:05:31 PM	This overview defines the scope of governance concern as it applies to security. It describes some of the top-level

7. daisy:568 (Adopting an Enterprise Software Security Framework)
8. daisy:564#wp1012117 (Governance and Management References)
9. daisy:194 (Architectural Risk Analysis)
10. daisy:60 (Assembly, Integration, & Evolution)
11. daisy:74 (Business Case Models)
13. daisy:65 (Measurement)
14. daisy:79 (Principles)
15. daisy:61 (Project Management)
16. daisy:68 (Risk Management)
17. daisy:80 (SDLC Process)
18. http://www.cert.org/podcast/

		considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Maturity of Practice and Exemplars	12/18/06 5:07:26 PM	This article identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.
Framing Security as a Governance and Management Concern: Risks and Opportunities	12/18/06 12:16:11 PM	This article briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs.
How Much Security Is Enough?	11/13/06 3:07:03 PM	This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.
Governance and Management References	11/9/06 5:06:50 PM	Content area bibliography.
Security Is Not Just a Technical Issue	11/9/06 5:05:31 PM	This overview defines the scope

		of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Framing Security as a Governance and Management Concern: Risks and Opportunities	12/18/06 12:16:11 PM	This article briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs.
Governance and Management References	11/9/06 5:06:50 PM	Content area bibliography.
How Much Security Is Enough?	11/13/06 3:07:03 PM	This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.
Maturity of Practice and Exemplars	12/18/06 5:07:26 PM	This article identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.

Security Is Not Just a Technical Issue	11/9/06 5:05:31 PM	This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.

Fields

Name	Value
Categories	best-practices